Claims

What is claimed is:

1. A method for allocating a resource, comprising the steps of:
   (a) receiving a resource allocation request from a client;
   (b) imposing on said client a computational task and a time limit for correct completion of said computational task;
   (c) receiving verification that said client has correctly performed said computational task within said time limit; and
   (d) allocating said resource for said client if the verification is received.

2. The method of claim 1 wherein said resource allocation request comprises a network connection request.

3. The method of claim 1 wherein said step (b) comprises communicating a puzzle as at least a portion of said communication task.

4. The method of claim 3 wherein said step (b) comprises communicating the output of a one-way function to said client.

5. The method of claim 3 wherein said step (b) comprises communicating the output of a block cipher to said client.

6. The method of claim 3 wherein said step (b) comprises communicating the output of a function, wherein the input of said function is generated, based at least in part on a server secret unknown to said client, and not revealed through correct performance of said computational task.

7. The method of claim 3 wherein said step (b) comprises communicating the output of a function, wherein the input of said function comprises a timestamp and information authenticating the timestamp.

8. The method of claim 3 wherein said step (b) comprises communicating a puzzle constructed in a self authenticating fashion.

9. The method of claim 3 wherein said step (b) comprises communicating a hash image and a partially revealed pre-image to said client.

10. The method of claim 9 wherein said step (c) comprises receiving the remaining pre-image.

11. The method of claim 3 wherein said step (b) comprises communicating a plurality of sub-puzzles to a client.

12. The method of claim 11 wherein said step (b) comprises communicating a plurality of independently constructed sub-puzzles.

13. The method of claim 11 wherein said step (b) comprises communicating a plurality of sub-puzzles wherein each sub-puzzle is constructed with some intended overlap.

14. The method of claim 1 wherein said step (a) comprises receiving a TCP SYN request.

15. The method of claim 1 wherein said step (a) comprises receiving a request to open an SSL connection.

16. The method of claim 1 wherein said step (b) comprises the steps of:

(ba) determining if a computational task is to be imposed upon said client based upon the operating circumstances at the time of receiving said resource allocation request from said client; and

(bb) if a computational task is determined to be imposed upon said client then selecting a computational task responsive to at least one characteristic of said operating circumstances at the time of receiving said resource allocation request; and

(bc) if a computational task is determined to be imposed upon said client then imposing the selected computational task on said client.

17. The method of claim 1, wherein said step (a) comprises receiving a resource allocation request comprising a query, or accompanied or preceded by a query concerning whether a server is currently imposing computational tasks.

18. A method for procuring a resource comprising the steps of:

(a) communicating a resource allocation request to a server;

(b) receiving a computational task from said server;

(c) performing or delegating the performance of said computational task correctly within a known time limit; and

(d) communicating to said server a verification that said computational task has been performed correctly within the known time limit.

19. The method of claim 18 wherein said resource allocation request comprises a network connection request.

20. The method of claim 18 wherein said step (b) comprises receiving said computational task and a time limit for performance of said computational task from said server.

21. The method of claim 18 wherein said step (c) comprises solving a puzzle.

22. The method of claim 21 wherein said step (c) comprises a linear search of the solution space associated with said computational task.

23. The method of claim 18 wherein said step (c) comprises solving a plurality of sub-puzzles.

24. The method of claim 18 wherein said step (a) comprises transmitting a TCP SYN request.

25. The method of claim 18 wherein said step (a) comprises transmitting a request to open an SSL connection.

26. The method of claim 18 wherein said step (a) comprises transmitting a resource allocation request comprising a query, or accompanied or preceded by a query concerning whether a server is currently imposing computational tasks.

27. A apparatus for allocating a resource comprising:
a first receiver receiving a resource allocation request from a client;
a computational task generator for imposing a computational task upon said client for correct performance within a time limit; and
a transmitter communicating said computational task to said client;
a second receiver receiving a verification from said client that said computational task was correctly performed with said time limit; and
an allocator allocating said resource for said client.

28. The apparatus of claim 27 wherein said first receiver and said second receiver comprise the same receiver.

29. The apparatus of claim 27 wherein said first receiver receives a resource allocation request comprising a network connection request.

30. The apparatus of claim 27 wherein said transmitter communicates said computational task and a time limit for performance of said computational task to said client;

31. The apparatus of claim 27 wherein said computational task comprises a puzzle.

32. The apparatus of claim 31 wherein said puzzle comprises the output of a one-way function.

33. The apparatus of claim 31 wherein said puzzle comprises the output of a block cipher.

34. The apparatus of claim 31 wherein said puzzle comprises the output of a function, wherein the input of said function is based at least in part on a server secret unknown to said client and not revealed through correct performance of said computational task.

35. The apparatus of claim 31 wherein said puzzle comprises the output of a function, wherein the input of said function comprises a timestamp and information authenticating the timestamp.

36. The apparatus of claim 31 wherein said puzzle is constructed in a self authenticating fashion.

37. The apparatus of claim 31 wherein said puzzle comprises a hash image, and a partially revealed pre-image.

38. The apparatus of claim 37 wherein said verification comprises verifying the remaining unrevealed pre-image.

39. The apparatus of claim 31 wherein said puzzle comprises a plurality of sub-puzzles.

40. The apparatus of claim 39 wherein said plurality of sub-puzzles are constructed independently.

41. The apparatus of claim 39 wherein said plurality of sub-puzzles are constructed with some intended overlap.

42. The apparatus of claim 27 wherein said resource allocation request comprises a TCP SYN request.

43. The apparatus of claim 27 wherein said resource allocation request comprises a request to open an SSL connection.

44. The apparatus of claim 27 wherein said computational task is selected responsive to at least one characteristic of the operating circumstances at the time of receiving said resource allocation request.

45. The apparatus of claim 27 wherein said resource allocation request comprises a query, or is accompanied or preceded by a query concerning whether a server is currently imposing computational tasks.

46. The apparatus of claim 27 comprising a time limit generator generating a time limit within which said client must correctly perform said computational task;

47. A apparatus for procuring a resource comprising:
a first transmitter communicating a resource allocation request to a server;
a first receiver receiving a computational task from said server;

a computational task solver correctly performing said computational task within a known time limit; and

a second transmitter communicating to said server a verification that said computational task has been performed.

48. The apparatus of claim 47 wherein said first transmitter and said second transmitter comprise the same transmitter.

49. The method of claim 47 wherein said first transmitter sends a resource allocation request comprising a network connection request.

50. The apparatus of claim 47 further comprising a second receiver receiving a time limit for performing said computational task.

51. The apparatus of claim 50 wherein said first receiver and said second receiver comprise the same receiver.

52. The apparatus of claim 47 wherein said computational task comprises a puzzle.

53. The apparatus of claim 47 wherein said computational task performs a linear search of potentially the entire solution space associated with said computational task.

54. The apparatus of claim 47 wherein said computational task comprises a plurality of sub-puzzles

55. The apparatus of claim 54 wherein said sub-puzzles are constructed independently.

56. The apparatus of claim 54 wherein said sub-puzzles are constructed with some intended overlap.

57. The apparatus of claim 47 wherein said resource allocation request comprises a TCP SYN request.

58. The apparatus of claim 47 wherein said resource allocation request comprises a request to open an SSL connection.

59. The apparatus of claim 47 wherein said resource allocation request comprises a query, or is accompanied or preceded by a query concerning whether said server is currently imposing computational tasks.